UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,465	05/11/2001	Geoffrey S. Strongin	2000.039500/TT3768	6696

23720 7590 11/15/2005

WILLIAMS, MORGAN & AMERSON, P.C.
10333 RICHMOND, SUITE 1100
HOUSTON, TX 77042

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/853,465	STRONGIN, GEOFFREY S.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-103* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-103* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: amendment filed on 24 August 2005, the original application was filed on 11 May 2001, with acknowledgement of continuing file date of 10 May 2001.

2. Claims 1-103 are currently pending claims 1, 32, 39, 51, 55, 64, 66, and 97 are independent claims. The amendment to the claims 16, 24, 31, and 81 for the addition of a period is accepted and corresponding objection withdrawn.

Response to Arguments

3. In response to applicants argument to the 112 Objection on page 3 *"In particular, the Examiner alleges that specification does not describe what data or secret is stored in the first location. Applicant respectfully submits that the use of secret information to protect confidential information is well-known. Furthermore, the secret information may take a variety of forms. Support for this position may be found in the references cited by the Examiner. See, e.g., Vu col. 1, ll. 11-33. Thus, Applicant respectfully submits that the specification does enable the use of a secret"*. The Office disagrees with argument as shown by applicant's own response the applicant's specification does not describe what secret is stored. The 112 rejection is maintained because the claims lack enablement.

In response to applicant's second argument on page 3, "Applicant respectfully submits that some embodiments of the present invention set forth techniques for accessing data stored in a first location using a secret. The content and/or the function of the access data are not material to the present invention". The Office disagrees with argument again Applicant's own response

shows the lack of enablement of the claimed invention. The claims and specification do not provide clear and concise understanding of the invention.

In response to applicant's argument on page 4, "Applicant respectfully submits that Vu fails to teach or suggest reading a secret from a first location, securing the secret in a secure location different from the first location, and retrieving at least a portion of the data stored in the first location using the secret, as set forth in independent claims 1, 51, 55, and 66. To the contrary, the physical token that originally stored the cryptographic key must be removed to ensure system integrity, thereby preventing the system from accessing any data stored on the physical token". The Office disagrees with argument, furthermore the argument does not make sense. The step of removing the token does not change that the secret and data stored in the first location is loaded into the secure operating system, hence the step of retrieving at least a portion of the data stored in the first location has already occurred by loading this information into the SMRAM. Furthermore the token could also still be available and the SMM mode could be initialized at another time see '104 col. 6, lines 6-21 "The cryptographic key and program may also be loaded after the system has already booted, as long as the loading is done in the secure mode, i.e. SMM. Also the cryptographic key and program may be loaded at different times. The program may be loaded during boot time, and the key at a later time. This implementation would be useful for computers which have multiple users and thus multiple keys, wherein all the keys rely on the exact same processing algorithm. The algorithm could be loaded at boot time, and the keys loaded later, as each user request security services". The references shows the claimed limitations, below is a more detailed mapping of independent claim 55. Applicant is

reminded the reference as a whole should be reviewed the sections cited in the reference are guides.

As to independent claim 55, "A method of securely accessing data in a personal computer" is disclosed in '104 col. 3, lines 53 through col. 4, line 35 "The present invention uses a special secure processing mode to process a cryptographic key provided on a token and an associated special secure memory area which is transparent to the operating system ... The following description of the preferred embodiment applies to the power-on sequence of a computer system ... Unlike a physical smart card, through, the token does not need to contain its own processor and accompanying hardware, since the processing will take place in the main system processor in a secure mode" (note "accessing data in a personal computer" is described in the above cited text, the token provides the cryptographic key which is used to access the secure memory contained within the computer system operating system);

"the method comprising: step for reading a secret from a first location" is shown in '104 col. 4, lines 11-17 "The following description of the preferred embodiment applies to the power-on sequence of a computer system ... the cryptographic key and programs can be loaded" (note reading has the same meaning as "loaded");

"step for securing the secret in a secure location different from the first location" is taught in '104 col. 4, lines 21-67 "Once the user's PIN is verified, the cryptographic key stored on the token is loaded into the System Management RAM (SMRAM) ... The SMRAM is then locked at step 7 which prevents any other processes from accessing the data stored in the SMRAM" (note the first location would be the token the second location would be the SMRAM);

"and step for retrieving at least a portion of the data stored in the first location using the secret" is disclosed in '104 col. 5, lines 30-47 "The SMI initializes the system processor into SMM. Once the processor is in SMM, a software SMI handler invokes the security function at step 22. The security function access the cryptographic key and programs stored in the SMRAM at step 23. The processor executes the requested security processing in the SMM. This processing may include encryption/decryption of documents, processing secret keys for password validation, user authentication, ect." (Note, the step of retrieving at least a portion the data stored in the first location occurs when the SMI call invokes the SMM. The step of retrieving a portion of the data using the secret has the same meaning of retrieving an algorithm and applying a key. Furthermore the data from the first location is loaded into the SMRAM the process of retrieving at least a portion of the data is invoked with SMI interrupt. As mentioned above this process can occur at any time. Finally the data in the first location and the second location are the same).

In response to applicant's second argument on page 4, "Applicant also submits that Vu fails to teach or suggest storing a secret within a first location and storing code different from the secret within the first location, where the code is configured to provide access to data stored in the first location when processed in association with the secret, as set forth in independent claims 32, 64, 97. The Office disagrees with argument, as stated above Vu disclosed using the data stored in the first location different from the secret (i.e. the algorithm) to access data stored in the first location when processed in association with the secret see '104 col. 5, lines 30-47 "The SMI initializes the system processor into SMM. Once the processor is in SMM, a software SMI handler invokes the security function at step 22. The security function access the cryptographic

key and programs stored in the SMRAM at step 23. The processor executes the requested security processing in the SMM. This processing may include encryption/decryption of documents, processing secret keys for password validation, user authentication, ect." (Note, the step of retrieving at least a portion the data stored in the first location occurs when the SMI call invokes the SMM. The step of retrieving a portion of the data using the secret has the same meaning of retrieving an algorithm and applying a key. Furthermore the data from the first location is loaded into the SMRAM the process of retrieving at least a portion of the data is invoked with SMI interrupt. As mentioned above this process can occur at any time. Finally the data in the first location and the second location are the same).

In response to applicants final argument on page 4, "Applicants also submits that Vu fails to teach or suggest a first location configured to store code, a secret, and data different from the secret and different from the code, and a master device operable coupled to the first location wherein the master device is configured to read the secret from the first location and store the secret in a secure location different from the first location, and wherein the master device is further configured to access the data stored in the first location using the secret as set forth in independent claim 39". The Office disagrees with argument as previously stated in addition the reference clearly states that algorithms can be loaded into the SMRAM. These algorithms are interpreted to have the same meaning as "data different from the secret and different from the code".

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1-103 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification as written does not describe what data or secret is contained in the first location. In addition the specification does not explain what function or use is performed when retrieving the data from the first location. In fact the initial pages of the specification describe a "System Management Mode (SMM)" operation, SMI, x86 processor, BIOS, and north/south bridge. None of these initial terms are in the independent claims.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-103 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In the claims there is no indication of what the secret is (i.e. a key, a code, a PIN, etc...) in addition there is no indication what the data contains or what function it performs.

8. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. 112 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

10. **Claims 1-103** are rejected under 35 U.S.C. 102(e) as being anticipated by Vu et al. U.S. Patent No. 6,557,104 (hereinafter '104).

As to independent claim 32, "A method of securing data in a personal computer system, the method comprising:" is taught in '104 col. 3, lines 53-67;

"storing a secret within a first location; and storing code different from the secret within the first location" is shown in '104 col. 4, lines 21-67;

"wherein the code is configured to provide access to data stored in the first location when processed in association with the secret" is disclosed in '104 col. 5, lines 30-47.

As to dependent claim 33, this claim contains substantially similar subject matter as claim 32 and is rejected along similar rationale.

As to dependent claim 34, "wherein the memory is a read-only memory (ROM); wherein storing a secret within the memory comprises storing a secret within the ROM; and wherein storing code different from the secret within the memory comprises storing code different within secret within the ROM; and wherein the code is configured to provide access to data stored in the ROM when processed in association with the secret" is shown in '104 col. 4, lines 21-67.

As to dependent claim 35, "wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM: configured to store the BIOS data; wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM; wherein storing code different within secret within the ROM comprises storing code different within secret within the BIOS ROM; and wherein the code is configured to provide access to BIOS data stored in the BIOS ROM when processed in association with the secret" is disclosed in '104 col. 4, lines 21-67.

As to dependent claim 36, "wherein storing a secret within the memory comprises storing the secret inside the data within the memory" is taught in '104 col. 4, lines 21-67.

As to dependent claim 37, "wherein storing a secret within the memory and storing code different from the secret within the memory comprises storing the secret inside the code within the memory" is taught in '104 col. 4, lines 21-67.

As to dependent claim 38, further comprising: providing a lock bit associated with the data stored in the memory that when set provides an indication that the data stored in the memory is secured" is shown in '104 col. 4, line 63 through col. 5, line 8.

As to independent claim 55, "A method of securely accessing data in a personal computer" is disclosed in '104 col. 3, lines 53-67;

"the method comprising: step for reading a secret from a first location; step for securing the secret in a secure location different from the first location" is taught in '104 col. 4, lines 21-67;

"and step for retrieving at least a portion of the data stored in the first location using the secret" is disclosed in '104 col. 5, lines 30-47.

As to dependent claim 56, "further comprising: step for reading code from the first location; wherein the code is different from the secret and different from the data stored in the first location" is taught in '104 col. 4, lines 21-67;

"wherein the step for retrieving at least the portion of the data stored in the first location using the secret comprises step for retrieving at least the portion of the data stored in the first location using the code and the secret" is disclosed in '104 col. 5, lines 30-47.

As to dependent claim **57, "further comprising: step for unlocking a lock bit associated with the data stored in the first location prior to the step for retrieving at least the portion of the data stored in the first location using the secret"** is taught in '104 col. 4, lines 21-67.

As to dependent claim 58, "further comprising: step for processing the secret using the code; wherein the step for unlocking the lock bit associated with the data stored in the first location comprises step for unlocking the lock bit associated with the data stored in the first location in response to the step for processing the secret using the code" is shown in '104 col. 5, lines 30-47.

As to dependent claim 59, "further comprising: step for storing the secret within the first location securely; step for storing data within the first location securely; and step for storing code different from the secret and different from the data within the first location securely" is disclosed in '104 col. 4, lines 21-67.

As to dependent claim 60, "further comprising: step for unlocking a lock bit associated with the data prior to the step for retrieving at least the portion of the data from the first location using the secret" is shown in '104 col. 4, lines 21-67.

As to dependent claim 61 and 62, these claims contain substantially similar subject matter as claim 55 and are rejected along the same rationale.

As to dependent claim 63, "further comprising: step for providing a lock bit associated with the data that when set provides an indication that the data stored in the first location is secured" is disclosed in '104 col. 4, lines 21-67.

As to independent claim 1, this claim contains substantially similar subject matter as claim 55 and is rejected along the same rationale.

As to dependent claim 15, this claim contains substantially similar subject matter as claim 59 and is rejected along the same rationale.

As to dependent claim 2, 16, 26, and 27, these claims contain substantially similar subject matter as claim 55 and are rejected along the same rationale.

As to dependent claim 17, "wherein the memory is a read-only memory (ROM); wherein storing a secret within the memory comprises storing a secret within the ROM; wherein storing data within the memory comprises storing data within the ROM; wherein storing code different from the secret and different from the data within the memory comprises storing code different within secret and different from the data within the ROM; wherein securing the secret in a secure location different from the memory comprises securing the secret in a secure location different from the ROM; and wherein retrieving at least a portion of the data from the memory using the secret comprises retrieving at least a portion of the data from the ROM using the secret" is taught in '104 col. 4, lines 21-67.

As to dependent claim 18, "wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data; wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM; wherein storing data within the ROM comprises storing data within the BIOS ROM; wherein storing code different within secret and different from the data within the ROM comprises storing code different within secret and different from the BIOS data within the BIOS ROM; wherein securing the secret in a secure location different from the ROM comprises securing the secret in a secure location different from the BIOS ROM; and wherein retrieving at least a portion of the data from the ROM using the secret comprises retrieving at least a portion of the BIOS data from the BIOS ROM using the secret" is shown in '104 col. 4, lines 21-67.

As to dependent claim 19, "wherein storing a secret within the memory and storing data within the memory comprises storing the secret inside the data within the memory" is disclosed in '104 col. 4, lines 21-67.

As to dependent claim 20, "wherein storing a secret within the memory and storing code different from the secret and different from the data within the memory comprises storing the secret inside the code within the memory" is taught in '104 col. 4, lines 21-67.

As to dependent claims 21 and 22, these claims are substantially similar to claims 56 and 57; therefore they are rejected along the same rationale.

As to dependent claim 23, "wherein reading the secret from the memory comprises reading the secret from the memory during a boot sequence; and wherein securing the

secret in a secure location different from the memory comprises storing the secret in SMM memory space" is shown in '104 col. 4, lines 21-67.

As to dependent claim 24, "wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises: processing the code; and transmitting at least an indication of the secret to the memory" is disclosed in '104 col. 4, lines 21-67.

As to dependent claim 25, "wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises: receiving a challenge from the memory; and transmitting a response to the memory including at least an indication of the secret to the memory, in response to receiving the challenge" is shown in '104 col. 4, lines 21-67.

As to dependent claim 3-14, these claims contain substantially similar subject matter as claims 17, 18, 19, 56, 61, 19, 57, and 58; therefore they are rejected along the same rationale.

As to dependent claim 28-31, these claims contain substantially similar subject matter as claims 23, 56, and 57; therefore they are rejected along the same rationale.

As to independent claim 39, this claim is directed to a computer system of the method of claim 55 therefore it is rejected along the same rationale.

As to dependent claims 40-49, these claims contain substantially similar subject matter as claims 17-20 and 55-63; therefore they are rejected along the same rationale.

As to dependent claim 50, "wherein the master device includes a microprocessor" is taught in '104 col. 4, lines 21-67.

As to independent claim 51, this claim is directed to a computer system of the method of claim 55 therefore it is rejected along the same rationale.

As to dependent claims 52-54, these claims contain substantially similar subject matter as claims 17-20 and 55-63; therefore they are rejected along the same rationale.

As to independent claim 64, this claim is directed to a computer system of the method of claim 32 therefore it is rejected along the same rationale.

As to dependent claims 65, this claim contains substantially similar subject matter as claim 38; therefore it is rejected along the same rationale.

As to independent claim 66, this claim is directed to a computer readable program of the method of claim 55 therefore it is rejected along the same rationale.

As to dependent claims 67-90, these claims contain substantially similar subject matter as claims 17-20 and 55-63; therefore they are rejected along the same rationale.

As to independent claim 97, this claim is directed to a computer readable program of the method of claim 32 therefore it is rejected along the same rationale.

As to dependent claims 98-103, these claims contain substantially similar subject matter as claims 33-38; therefore they are rejected along the same rationale.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
8 November 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100